



Europäisches Patentamt
European Patent Office
Office européen des brevets

EP 168 212 A1



EUROPEAN PATENT APPLICATION

(43) Date of publication:

02.01.2002 Bulletin 2002/01

(51) Int. Cl.7: G06F 17/60

FIELD OF THE INVENTION

1 EP 168 212 A1

2

has its object to provide an assets management method and system for enabling low-cost, highly-flexible, highly-reliable, efficient and safe assets risk management and earnings management, for geographically distributed users or managed assets data.

[0009] According to the present invention, the foregoing object is attained by providing an assets management method comprising the steps of: managing access of users to resources by providing history authentication management means for managing histories for users of managed assets and performing authentication management, in a risk and earnings management apparatus which generates data on risk management and earnings management by calculating input users data, and enabling an unlimited number of users to access the risk and earnings management apparatus via a network.

[0010] The history authentication management means provides authorization to utilize the resources in the risk and earnings management apparatus based on user or managed assets.

[0011] Further, data transmitted between the user and the risk and earnings management apparatus via the network is encrypted for security purposes.

[0012] Further, the foregoing objects are attained by providing an assets management system including a risk and earnings management apparatus which generates data on risk management and earnings management by calculating input assets data and a user terminal which accesses the risk and earnings management apparatus via a network, comprising: history authentication management means, provided in the risk and earnings management apparatus, for managing histories for users or managed assets and performing authentication management, thereby managing access of user resources, wherein an unlimited number of users are enabled to access the risk and earnings management apparatus via a network.

[0013] Note that the history authentication management means provides authorization to utilize the resources in the risk and earnings management apparatus based on user or managed assets. Further, data transmitted between the user and the risk and earnings management apparatus via the network is encrypted in accordance with level of security desired.

[0014] Further, the foregoing object is attained by providing a risk and earnings management method comprising: data management means for storing and searching for input/output data for respective users or managed assets, calculation processing means for processing the input data and obtains output data; history authentication management means for managing histories for the users or managed assets and performing authentication management, and network connection management means for performing flow control, data encryption and data compression/decompression.

[0015] Note that the history authentication management means provides authorization to utilize the resources in the risk and earnings management apparatus.

2

SUMMARY OF THE INVENTION

[0008] The present invention has been made to remove the drawbacks of the above conventional art, and

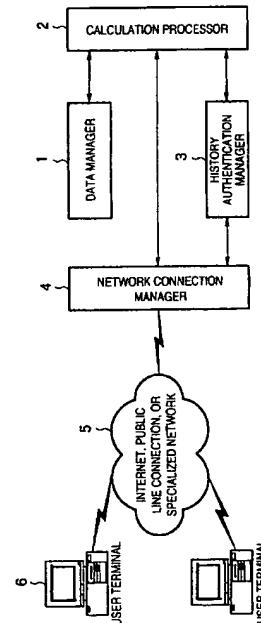


FIG. 1

3	EP 1 168 212 A1	4	
5	EP 1 168 212 A1	6	
	DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT		
[0023]	bus based on user or managed assets. Further, the network connection management means encrypts data transmitted between the user and the risk and earnings management apparatus via the network in accordance with a level of security defined.	[0024]	Further, in a case where a portfolio logic, including various theories and different approaches such as value-at-risk (VaR), risk return analysis and portfolio optimization, are employed, functions based on different methods and/or standards can be independently provided to the respective users or managed assets as different systems are operated based on history authentication information for the respective user or managed assets.
[0016]	Further, the foregoing object is attained by providing an computer-readable storage medium holding a control program for controlling risk and earnings management apparatus which generates data on risk management and earnings management by calculating input assets data, wherein the control program comprising: a data management program for storing and searching for input/output data for respective users or managed assets; a calculation processing program for processing the input data and obtains output data; a history authentication management program for managing histories for the users or managed assets and performing authentication management; and a network connection management program for performing flow control, data encryption and data compression/decompression.	[0025]	In addition, in a case where functional improvement and revision are continuously made, correction can be made on the side of centralized risk and the earnings management apparatus side while keeping the graphically distributed user terminals unchanged. Accordingly, the costs of functional maintenance and revision can be reduced.
[0018]	The history authentication management program includes a step of providing authorization to utilize the resources in the risk and earnings management apparatus based on user or managed assets. Further, the network connection management program includes a step of encrypting data transmitted between the user and the risk and earnings management apparatus via the network in accordance with a level of security desired.	[0026]	Other features and advantages of the present invention will be apparent from the following description taken in conjunction with the accompanying drawings, in which like reference characters designate the same name or similar parts throughout the figures thereof.
	BRIEF DESCRIPTION OF THE DRAWINGS		
[0019]	The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate embodiments of the invention and, together with the description, serve to explain the principles of the invention.	[0027]	Fig. 1 is a block diagram showing an example of the hardware construction of the assets management system according to an embodiment of the present invention; Fig. 2 is a block diagram showing an example of the hardware construction of the assets management system according to the embodiment.
[0018]	Further, the present invention provides versatility and security for input/output of large amount of data even in use of small-capacity line, by compressing and encrypting data transmitted between the system and the user terminal, and assigning an authentication key to each user or managed assets.	[0028]	Fig. 3 is an explanatory view showing an example of the construction of a history authentication key DB according to the embodiment;
[0019]	Further, the present invention provides memory areas to respective users or managed assets, extracts and provides output results based on methods and/or standards depending on the respective users or managed assets.	[0029]	Fig. 4 is a block diagram showing an example of the construction of a data management DB according to the embodiment;
[0020]	Further, the present invention realizes simple functional revision and low maintenance cost by providing a management apparatus, not on the side of geographically distributed on plural users, but in a centralized location.	[0030]	Fig. 5 is a schematic diagram showing an example of the construction of a calculation processing program according to the embodiment;
[0021]	As described above, according to the present invention, efficient and safe assets risk management and earnings management can be realized even for geographically distributed users and managed assets data.	[0031]	Fig. 6 is a flowchart showing an example of a processing procedure in a risk and earnings management apparatus according to the embodiment;
[0022]	Accordingly, assets risk management and earnings management can be realized via a low-cost network line for e.g. the Internet access even for major corporations having a large amount of data and financial institutions handling secret financial data including cus-	[0032]	Fig. 7 is a flowchart showing an example of a processing procedure of history authentication processing in Fig. 6;
		[0033]	Fig. 8 is a flowchart showing an example of a processing procedure of calculation processing in Fig. 6.

the network line 5 between the memory and the network connection manager 4 of the risk and earnings management apparatus; 15, the various control display programs for various control displays on the user terminal; and 16, an assets data memory for temporarily storing data before the data is sent via the network line 5 to the data manager 1.

<Example of History Authentication Construction>

[0037] Fig. 3 shows an example of the construction of the history authentication key DB 3a.

[0038] Data transmitted by the user terminal 6 includes at least a terminal ID, a user ID (including a password and the like) and a history authentication key, and on the basis of these IDs and key, terminal IDs 31, user IDs 32 and history authentication keys 33 on the history authentication key DB 3a.

[0039] In Fig. 3, input data A, C and D are used, and use of data B is limited. In the calculation processing, commands a, b and d are processed but a command c is not processed. Among the results of calculation, output data 1 and 3 are outputted (returned to the user terminal) but output data 2 is not outputted. Note that if it is arranged such that especially commands are hierarchically limited with limitation by dividing one processing method for plural commands, and by selecting one processing method from plural processing methods or selecting one specific processing method in correspondence with input data or output format, a system can be constructed with greater general versatility. Furthermore, a more general system sharing the resources can be constructed. In this case, the attainment of security by history authentication of the present invention becomes a more important function.

[0040] Note that, in Fig. 3, the input data, commands and the output data are clearly separated for the purpose of simplification, however, a method of constructing a hierarchical structure and control use of levels of the structure, a method of controlling masking/not mask-

ing a part of data can be performed, and regarding command processing, control by argument, i.e., control by the difference of parameters or branch/destination used in the program, can be performed. Further, a limit of the number of significant digits of data, a limit of the width of convergence in calculation, and a limit by replacing a pair of data with blank or omission, upon output, can be made. In the present embodiment, the use of resources and services are limited in correspondence with user in consideration of a possibility that sensitive data such as corporation secret and customer secret are handled via the internet or the like when the present system is published. The range of publicity can be widened with increase in reliability of the security.

[0041] Fig. 4 is a block diagram schematically showing an example of the construction of the data management database (DB) 1b or input data management. Numerals 41 to 44 denote contents of input data A to D. Note that the input data is not always clearly separated as shown in the figure, but generally, the input data A to D overlap each other. Actually, the database is hierarchically structured or divided in a complicated manner. Although Fig. 4 does not show output data as the results of calculation, the output data is stored in the data management database (DB) 1b, and thereafter, the data is also used as input data. In this case, all the necessary data are stored regardless of the limit of output data in Fig. 3.

[0042] As shown in Fig. 4, the data areas 41 to 44 respectively have a header and data. In the header, as a history authentication key, when who registered the data, or whom the user can show the data security (owner or the data, or whom the user cannot show the security level or the data, are described upon registration or update). The key increases the security in cooperation with the above input limits in Fig. 3. Note that it may be arranged such that one of the history authentication keys in Figs. 3 and 4 is used in correspondence with the security of the database.

[0043] Fig. 5 is a schematic diagram showing an example of the construction of the calculation processing program 2. Fig. 5 shows command a processing 51, to command d processing 54. As in the case of Fig. 4, the command processing programs 51 to 54 respectively have a header where conditions of use of processing program, processing precision upon use and information on processing method are described.

[0044] Note that, the limitation of the calculation processing in Fig. 3 is an example, and the calculation processing program 2 is not necessarily limited in correspondence with the command. For example, the limitation is indicated by the arguments of the respective programs, and the number of calculations in the Monte Carlo method or the like is limited. As a particular example of the program argument control, a Monte Carlo method in conformity with discrete probability density function and a Monte Carlo method in conformity with

continuous probability density function are prepared and users or the range of both methods are limited by the program arguments.

[0045] Further, in Fig. 3, all the input data, the calculation processing and the output data are limited, however, it may be arranged such that only the output data is limited and all the necessary input and calculation are performed inside and the results are stored in the data management database (DB) 1b. In this case, the output data returned to the user terminal is masked in accordance with limitations. For example, if data where a company name, a customer name or non-parsable data is replaced with omission, and the data returned to be displayed, business effects can be expected.

<Example of Operation of Assets Management System of Present Embodiment>

[0046] Hereinbelow, an example of the operation of assets management system, according to the present embodiment will be described. Note that the operation at the user terminal 6, transaction via the network, the data compression and encryption and the like are not main parts of the present invention, and therefore detailed description about them will be omitted.

[0047] Fig. 6 is a flowchart showing the entire processing in the risk and earnings management apparatus according to the present embodiment.

[0048] The risk and earnings management apparatus walls for the user terminal 6 at step S10. Upon reception of request data from the user terminal 6 is received at step S20. At this time, data decryption and decompression and the like are also performed. Note that it is preferable that one of several different types of encryption is performed in correspondence with security, or plural encryption is performed on high secret data based on the content of data. Especially, assets data must be prevented from leaking to the outside, accordingly, the most strict encryption is performed on the assets data with the company name and the customer name. Similarly, the most strict encryption is performed on risk and earnings management data to be returned.

[0049] At step S30, the "authorization" data as the result of calculation processing is limited in accordance with the "authorization" data. At step S44, the calculation processing is performed to obtain the assets variation and the risk management data within the limitation of the input data and the calculation processing. At step S42, the "authorization" data as the result of calculation in accordance with the "authorization" data, and the information is outputted.

[0050] As many apparently widely different embodiments of the present invention can be made without departing from the spirit and scope thereof, it is to be understood that the invention is not limited to the specific embodiments thereof except as defined in the appended claims.

Claims

51. An assets management method comprising the steps of:

managing access of user resources by provid-

ence with user is also applied to the display format) or the difference of parameters or branch/destination used in the program arguments. Further, at step S31, the terminal ID and the user ID are obtained from the data sent from the user terminal 6. As described above, the terminal ID is not used in many cases. Next, at step S32, the history authentication key is obtained. At step S33, based on the obtained terminal ID, the user ID and the history authentication key, the "authorization" of the user is determined (See Fig. 3). At step S34, it is determined whether or not the obtained "authorization" is to be changed, and if NO, the process jumps to step S36, at which data indicating the "authorization" is forwarded to the calculation processing program. If it is determined at step S34 that the "authorization" is to be changed, the "authorization" is changed at steps S35, and the changed "authorization" is forwarded to the calculation processing program at step S38. Note that the "authorization" can be changed at any time in correspondence with a slight change based on the relation among financial institutions, a change in business amount, the period of business and the like. Accordingly, the "authorization" may be limited due to the degradation of credit level. Further, it may be arranged such that the "authorization" is fixed to the user ID or history authentication key, and the user ID or history authentication key is changed upon renewal of contract.

[0051] Fig. 7 is a flowchart showing an example of the calculation processing at step S40 in Fig. 6. In this example, all the input data, calculation processing and output data are limited.

[0052] First, at step S41, the "authorization" data as the result at step S30 is obtained. At step S42, the input data is limited in accordance with the "authorization" data. At step S43, the calculation processing is limited in accordance with the "authorization" data. At step S44, the calculation processing is performed to obtain the assets variation and the risk management data within the limitation of the input data and the calculation processing. At step S45, information is selected or masked by the result of calculation in accordance with the "authorization" data, and the information is outputted.

[0053] As many apparently widely different embodiments of the present invention can be made without departing from the spirit and scope thereof, it is to be understood that the invention is not limited to the specific embodiments thereof except as defined in the appended claims.

11 EP 1 68 212 A1 12 calculation processing means for processing the input data and obtains output data; history authentication management means for managing histories for the users or managed assets and performing authentication management in a risk and earnings management apparatus which generates data on risk management and earnings management by using input assets data; and enabling an large number of users to access said risk and earnings management apparatus via a network.

10 2. The assets management method according to claim 1, wherein said history authentication management means provides authorization to utilize the resources in the risk and earnings management apparatus based on user or managed assets.

15 3. The assets management method according to claim 1, wherein data transmitted between said user and earnings management apparatus via the network is encrypted in accordance with level of security desired.

10 4. An assets management system including a risk and earnings management apparatus which generates data on risk management and earnings management by calculating input assets data and a user terminal which accesses said risk and earnings management apparatus via a network, comprising: history authentication management means, provided in said risk and earnings management apparatus, for managing histories for users or managed assets and performing authentication management, thereby managing access of user resources, wherein an unlimited number of users are enabled to access said risk and earnings management apparatus via a network.

20 5. The assets management system according to claim 4, wherein said history authentication management means provides authorization to utilize the resources in the risk and earnings management apparatus based on user or managed assets.

15 6. The assets management system according to claim 4, wherein data transmitted between said user and said risk and earnings management apparatus via the network is encrypted in accordance with level of security desired.

10 7. A risk and earnings management apparatus comprising: data management means for storing and searching for input/output data for respective users or managed assets,

25 8. The risk and earnings management apparatus according to claim 7, wherein said network connection management means encrypts data transmitted between said user and said risk and earnings management apparatus via the network in accordance with level of security desired.

30 9. The risk and earnings management apparatus according to claim 7, wherein said network connection management means provides authorization to utilize the resources in the risk and earnings management apparatus based on user or managed assets.

35 10. A computer-readable storage medium holding a control program for controlling a risk and earnings management apparatus which generates data on risk management and earnings management by calculating input assets data, wherein said control program comprising: a data management program for storing and searching for input/output data for respective users or managed assets; a calculation processing program for processing the input data and obtains output data, a history authentication management program for managing histories for the users or managed assets and performing authentication management; and a network connection management program for performing flow control, data encryption and data compression/decompression.

40 11. The storage medium according to claim 10, wherein said history authentication management program includes a step of providing authorization to utilize the resources in the risk and earnings management apparatus based on user or managed assets.

45 12. The storage medium according to claim 10, wherein said network connection management program includes a step of encrypting data transmitted between said user and said risk and earnings management apparatus via the network in accordance with level of security desired.

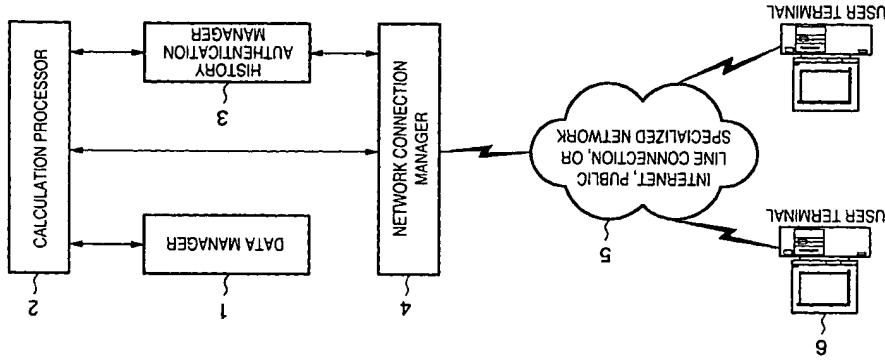
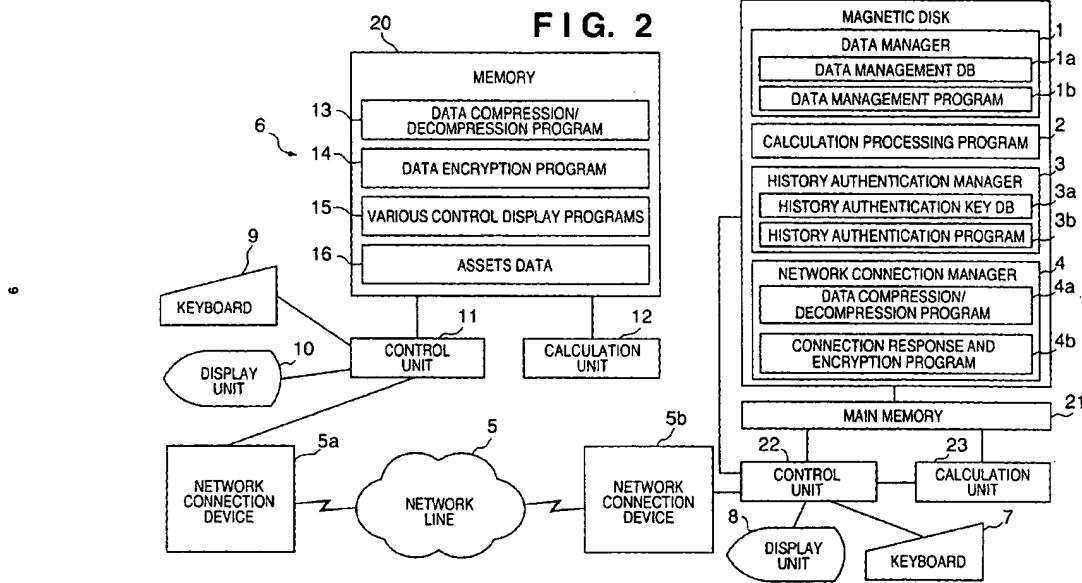


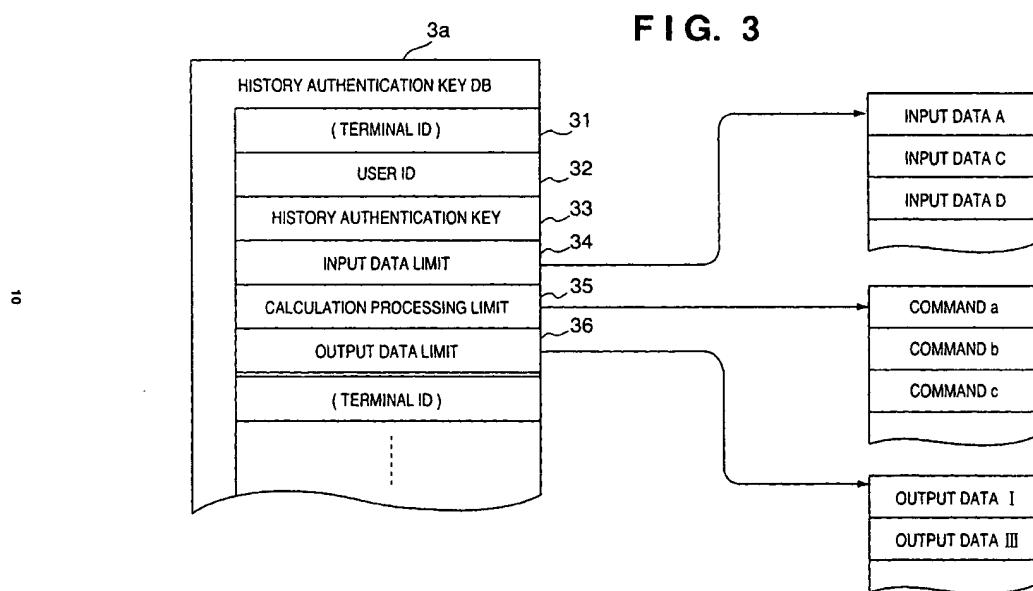
FIG. 1

FIG. 2



EP 1 168 212 A1

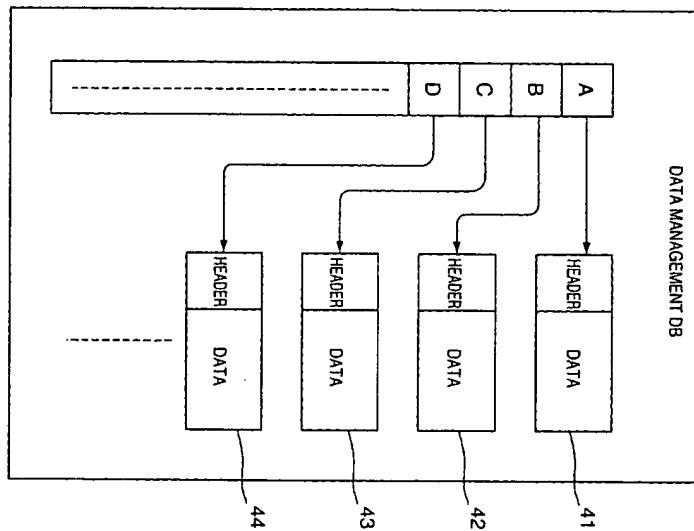
FIG. 3



EP 1 168 212 A1

FIG. 4

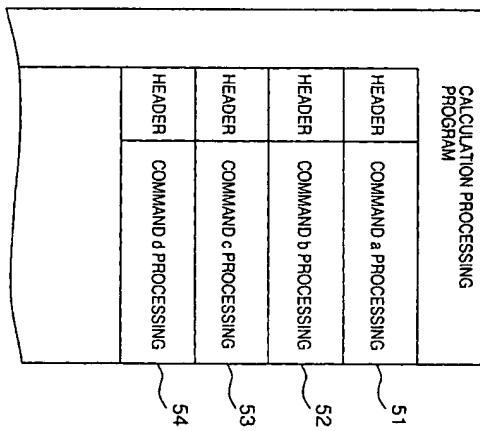
1b



11

FIG. 5

2



12

FIG. 6

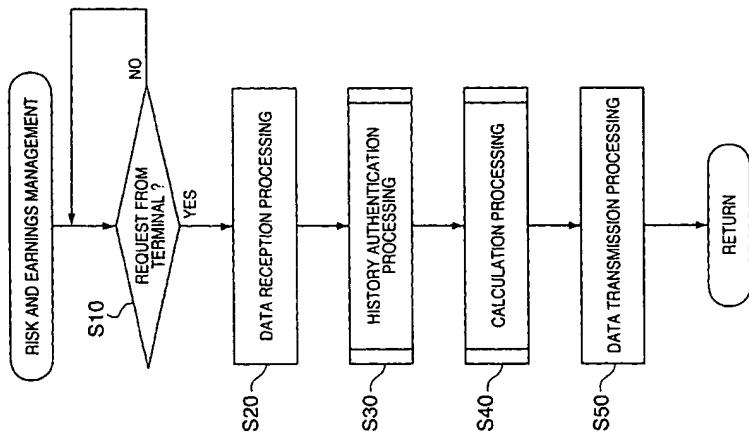


FIG. 7

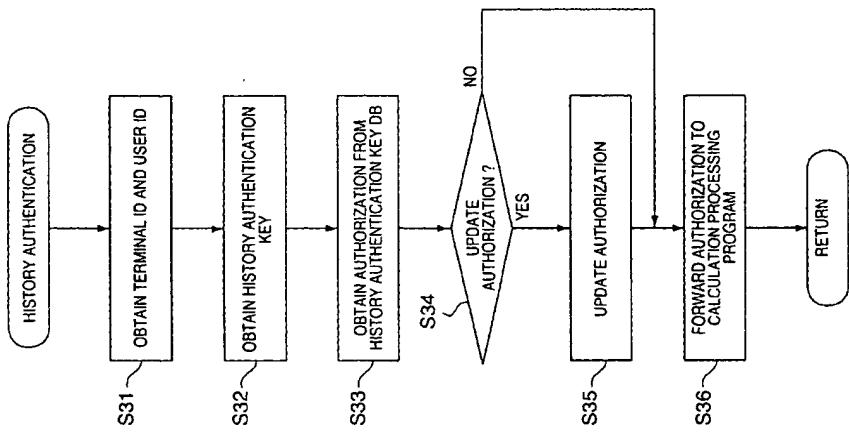
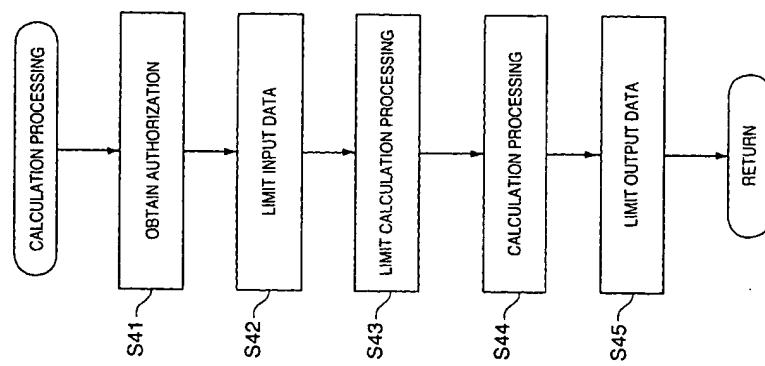


FIG. 8



European Patent Office	Application Number which under Rule 45 of the European Patent Convention EP 01 16 7743 shall be subscribed, for the purposes of subsequent proceedings, as the European search report
Reason:	
<p>The Search Division considers that the present application does not comply with the provisions of the EPC in such an extent that it is not possible to carry out a meaningful search into the state of the art on the basis of all claims.</p> <p>The Search Division considers that the subject-matter claimed in claims 1-3 fails under the provisions of Article 52(2) and (3) EPC, such subject-matter relating to a method of doing business as such.</p> <p>Claims 4-14 relate to commonplace technological features for performing the business method of the method claims. Although these claims do not literally belong to the method category, they essentially claim protection for the same commercial effect as the method claims. With reference to the Guidelines, B-VII, points 1-6, the Search Division considers that searching such commercial features would serve no useful purpose. This applies to the remaining commonplace technological features of these claims as well.</p> <p>The applicant's attention is drawn to the fact that a search may be carried out during examination following a declaration of no search under Rule 45 EPC, should the problems which led to the declaration being issued be overcome (see EPC Guideline C-VI, 8.5).</p>	
CLASSIFICATION OF THE APPLICATION (if any)	
606F17/60	
EPO-REF-168-212-A1	
Place & Date	14 September 2001
THE HAGUE	Nicoli, F